AB:DEL

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF THE PREMISES KNOWN AND DESCRIBED AS 17 MEADOW STREET, GARDEN CITY, NEW YORK, 11530 AND ANY CLOSED CONTAINERS/ITEMS CONTAINED THEREIN

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT
OF A SEARCH WARRANT

No. 19-1161 M

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Krista Cousins, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 17 Meadow Street, Garden City, New York, 11530 (the "SUBJECT PREMISES"), further described below and in Attachment A, for the things described in Attachment B.

3. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been since December 2017. I am currently assigned to the Child Exploitation Investigations Unit. During my tenure with HSI, I have participated in investigations targeting individuals involved in the receipt, distribution and possession of child pornography and have conducted physical and electronic surveillance, executed search warrants, reviewed and analyzed electronic devices, and interviewed witnesses. As part of my employment with HSI, I successfully completed the Federal Law

Enforcement Training Center's Criminal Investigator Training Program and Immigration and Customs Enforcement Special Agent Training, both of which included instruction with respect to the application for, and execution of, search and arrest warrants, as well as the application for criminal complaints, and other legal processes. As part of my responsibilities, I have been involved in the investigation of child pornography cases and have reviewed photographs depicting children (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor.

2. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251 (sexual exploitation of children), 2252 and 2252A (activities relating to material constituting or containing child pornography), and/or 2423 (travel with intent to engage in illicit sexual conduct) (collectively, the "SUBJECT OFFENSES") have been committed by TOM BLAHA.

3. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from my own personal participation in the investigation, my review of documents, my training and experience and discussions I have had with other law enforcement personnel concerning the creation, distribution and proliferation of child pornography. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

7. In or about November 2019, HSI received information from the National Center for Missing and Exploited Children ("NCMEC") indicating that a Facebook account belonging to an individual named TOM BLAHA ("BLAHA") had communicated with another Facebook account belonging to an apparent minor located in the Philippines (the "Victim"), and that such communications reflected the apparent enticement of a minor to engage in sexual activity, travel from the United States to the Philippines to engage in sexual activity with a minor, and the creation and sale of child pornography. The information received from the NCMEC included details relating to the accounts such as user name, ID number, e-mail address and IP addresses used to access the Facebook accounts.

8. The account belonging to BLAHA has the unique user ID "1132805002" (the "BLAHA ACCOUNT"). The information received from the NCMEC indicates that the BLAHA ACCOUNT connected to the Internet from different locations within Long Island, New York on October 8, 2019, and October 9, 2019. The BLAHA ACCOUNT also connected to the Internet from Manila, Philippines, on or about October 17, 2019. The BLAHA ACCOUNT is registered to an individual with a given username of "Tom Blaha," a date of birth of April 1, 1956, and an e-mail address of tom_blaha@msn.com.

9. The account belonging to the apparent minor located in the Philippines has the unique user ID "100011740475726" (the "Victim Account"). The information received from the NCMEC indicates that the Victim Account connected to the Internet from Manila, Philippines on November 25, 2019. The Victim Account is registered to an individual with a

date of birth of May 5, 1999. However, based on the facts described below, there is reason to believe that the Victim is a minor.

10. Customs documents and passport records indicate BLAHA traveled to the Philippines on or about September 14 to September 26, 2019, and October 10 to October 26, 2019.

11. Based on messages exchanged between the accounts, which the NCMEC received and then forwarded to HSI, it appears that BLAHA and the Victim had met in person and engaged in sexual activity at least once before September 20, 2019, in exchange for money. For example, on September 20, 2019, BLAHA called the Victim his "girlfriend" and said she was the "World[']s best kisser." The Victim responded that she "got [her] money baby thank you so much," and BLAHA wrote back, "Your welcome my lover."

12. On or about September 23, 2019, BLAHA and the Victim discussed the Victim creating sexually explicit videos to send to BLAHA in exchange for money. Specifically, the Victim wrote, "My sister has offer on me she said you want me to make 3 video[s] with vibrator. I agree with her but can you make 30k for that it[']s [hard] for me." BLAHA wrote back, "Ok my love . . . Make me happy." Based on my training and experience, I believe the reference to "30k" means 30,000 Philippine pesos, which are worth approximately $600.

13. During BLAHA's trip to the Philippines in October 2019, BLAHA appears to have met the Victim and have engaged in sexual activity. For example, on or about October 4, 2019, BLAHA wrote to the Victim that he loved and missed her, that he would see her in

two weeks, and that he "want[s] to pet it." Then, on or about October 17, 2019, the following exchange occurred:[1]

Victim Account:	hi baby is it ok if we resdule our meeting tomorrow because im busy on 19 to my school???
BLAHA ACCOUNT:	Can you send me a few mirror pictures in underwear?
BLAHA ACCOUNT:	Babe, 130,000 pesos without fuck or 200,000 pesos with fuck??
. . .	
Victim Account:	200 pesos can do everything baby but no sex baby pls in not ready yet…
BLAHA ACCOUNT:	So you choose 130,000 pesos, everything but fuck, that's fine
. . .	
BLAHA ACCOUNT:	See you later lover!! Shave your pussy, ok?

14. After BLAHA left the Philippines in October 2019, he wrote to the Victim that he would come back in January. He also referred to sending money to the bank account of the Victim's sister for the benefit of the Victim, which may indicate that the Victim is not old enough to have her own bank account. Specifically, on or about October 18, 2019, the following exchange occurred:

BLAHA ACCOUNT:	I promise to think of you everyday till I come back in January

[1] Verbatim exchanges described herein are comprised of excerpts from a longer message thread. Gaps between excerpts are denoted with ellipses.

Victim Account:	me too baby and thank you a lot
Victim Account:	baby when did i got my money hope you dont mind i need for my mom…
BLAHA Account:	I can send to your sisters bank like last time, takes a few days for international processing

15. Based on information and belief, the Victim is under the age of 18. On or about December 2, 2019, HSI agents reviewed the Victim Account, which is publicly accessible and contains a large number of photographs of a young female who is the apparent owner of the account – i.e., the Victim. Based on the physical appearance of the individual depicted in those photos, the Victim is well under the age of 18 and may be as young as 13 or 14. Furthermore, in certain of the photos, the Victim is wearing a school uniform that appears to be consistent with those often worn by students in middle school or high school. On April 5, 2019, the Victim posted a "Certificate of Achievement" from an elementary school in the Philippines, indicating she is 14 years old or younger.

16. On or about December 5, 2019, HSI agents reviewed publicly accessible video clips posted by the Victim on Facebook and other social media platforms, showing the Victim in classrooms or other school settings. In those videos, there are many children that appear to be between approximately 6 and 13 years of age. Both the Victim and those children are wearing similar uniforms in the videos.

17. The Honorable Sanket J. Bulsara signed a search warrant authorizing a search of the Facebook accounts of BLAHA and the Victim from the time period of January 1, 2019,

to the present. See Case No. 19-1141M (Bulsara, J.) (signed December 6, 2019). The records obtained from Facebook revealed:

a. A fully nude photograph of the Victim that BLAHA sent to another Facebook user on or about September 22, 2019;

b. A screenshot of a wire transfer BLAHA sent to the victim's sister at her account in the Bank of Philippine Islands, Makati Metro Manila, Manila Philippines, for 175,000 Philippine pesos on or about October 22, 2019. In a conversation with the Victim's sister, BLAHA noted, "130K is for [Victim]." Based on my training and experience, I believe the reference to "130k" means 130,000 Philippine pesos, which are worth approximately $2,500; and

c. Photographs of BLAHA, the Victim, and the Victim's sister in September 2019 in the Philippines.

18. Furthermore, in addition to the Victim, BLAHA has sent and received other images on the BLAHA ACCOUNT of girls, who in my training and experience, appear to be minors in sexually explicit images, including:

a. On or about September 21, 2019, BLAHA sent a photograph to another Facebook user which depicts an unidentified female, who appears to be approximately 14 to 17 years old based on her physical development and that she has braces on her teeth. She is photographed from the waist up and is wearing a fishnet top that exposes her breasts.

b. On or about September 26, 2019, BLAHA sent two photographs to another Facebook user. The first depicts an unidentified female victim lying on a bed in a black bra and thong underwear. Based on her physical development she appears to be approximately 14 to 17 years old. The second photograph depicts an unidentified female from the neck down. She is standing in a shower stall, fully nude. Based on her physical development she appears to be approximately 13 to 16 years old.

19. HSI served a subpoena to Optimum ("Optimum") for the IP information provided by Facebook for the BLAHA ACCOUNT from the time period of October 8, 2019 and October 9 2019, corresponding to activity on the BLAHA ACCOUNT provided in the NCMEC report. Records obtained by Optimum reveal that the BLAHA ACCOUNT was accessed from an IP Address 24.189.120.182, which lists the subscriber of record as RICHARD ROGERS and corresponds to the physical address of 17 Meadow Street, Garden City, New York.

20. Based on information, including publicly available records, indicate BLAHA resides alone at SUBJECT PREMISES. For instance:

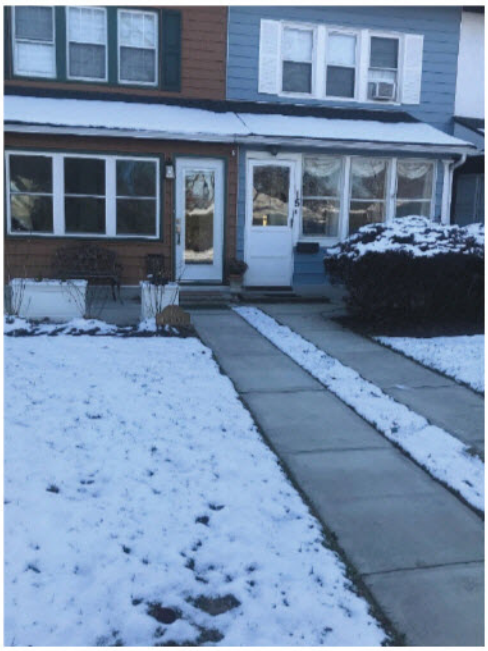
a. The deed to the SUBJECT PREMISES lists BLAHA as the sole owner of the property as of January 2018;

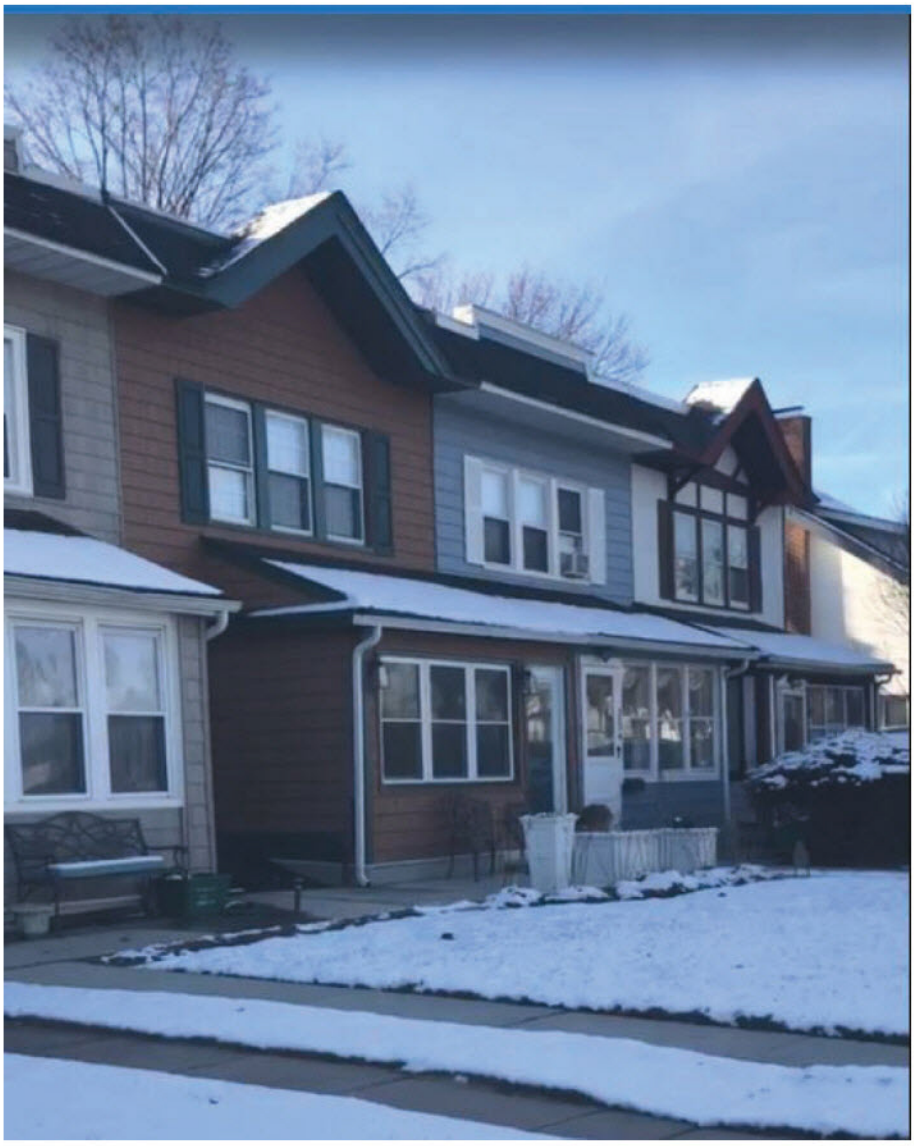
b. Open-source records indicate BLAHA is not married, and while he has at least one son, that son does not reside with him; and

c. BLAHA listed the address for the SUBJECT PREMISES on customs documents upon his return to the United States as recently as September 26, 2019.

THE SUBJECT PREMISES

7. The SUBJECT PREMISES, which is located at 17 Meadow Street, Garden City, New York, 11530, is a single-family attached two-story row home, depicted in the photographs below. There is dark brown siding and dark-colored shutters. There is a concrete walkway and one step leading to the main entrance. The main entrance is a full-length glass-paned door trimmed in white with a gold-colored handle and door lock. There are two concrete planters in front of the home. There is no number on the premises but the odd-numbered units are sequential.





CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

8. Further, based on my training and experience and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child

pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing websites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

9. I know that collectors of child pornography typically retain their materials and related information for many years.

10. I also know that collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

11. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

12. Based on my experience, I know that persons who collect and distribute child pornography frequently collect and view sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification. These examples of visual media containing sexually explicit materials are often times stored on various devices, including but not limited to, computers, disk drives, modems, thumb drives, personal digital assistants, mobile phones and smart phones, digital cameras, and scanners, and the data within the aforesaid objects relating to said materials.

DEFINITIONS

13. The following definitions apply to this Affidavit and the attachments to this Affidavit:

a. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)). The terms "minor," "sexually explicit conduct" and "visual depiction" are defined as set forth in Title 18, United States Code, Section 2256.

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

c. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of

the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

d. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[.]"

e. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); and peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as modems, routers, cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way

they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Hash value" refers to a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated.

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP

assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. "Domain name" is a name that identifies an IP address.

j. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, drives, or electronic notebooks and tablets, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

14. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of

electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

15. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

16. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information

on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and

storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime

(e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

17. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software,

and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

19. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

20. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Special Agent Krista Cousins
Homeland Security Investigations

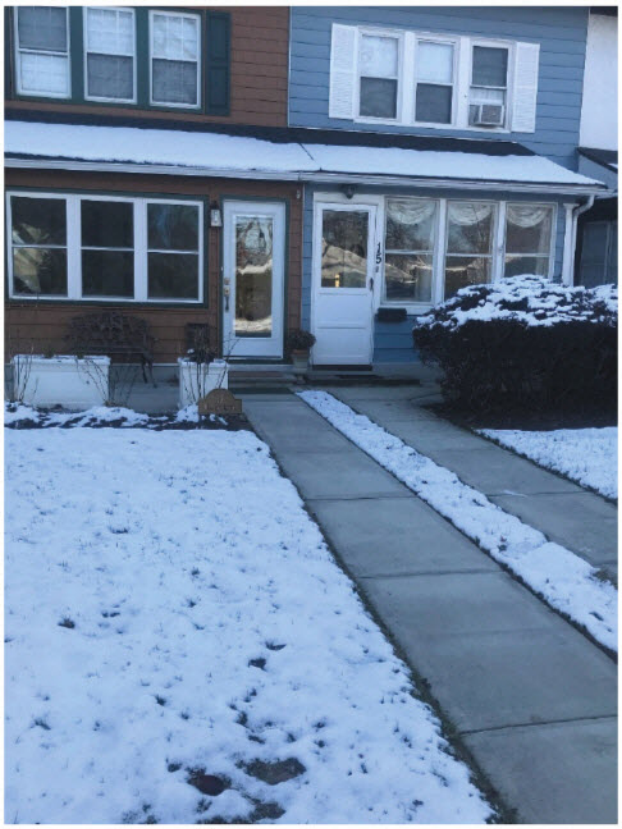
Subscribed and sworn to before me
on December 13, 2019:

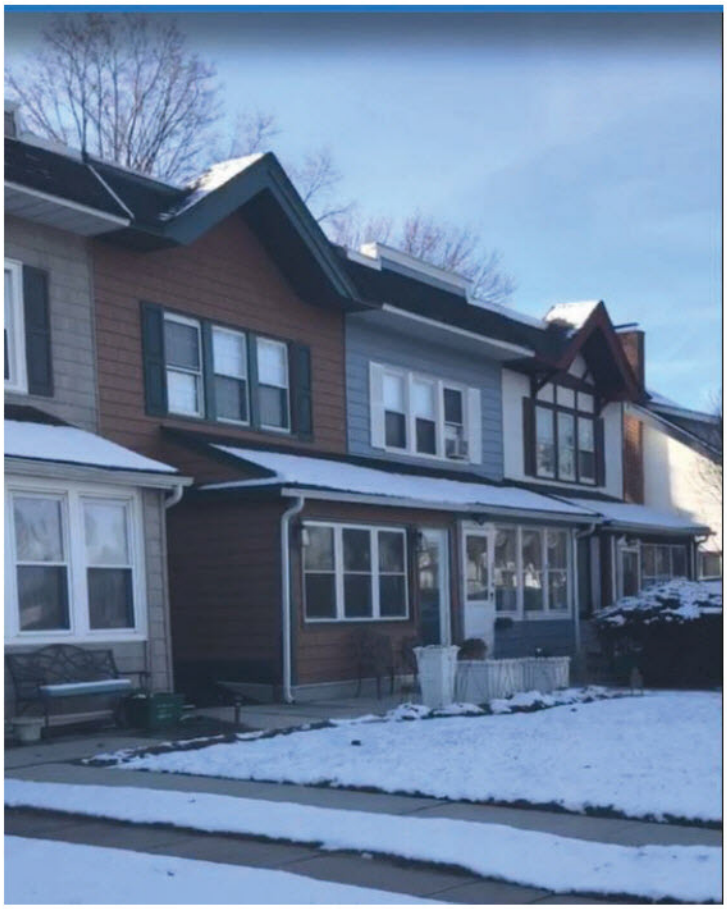
HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The SUBJECT PREMISES is 17 Meadow Street, Garden City, New York, 11530, which is a single-family attached two-story row home, depicted in the photographs below. There is dark brown siding and dark-colored shutters. There is a concrete walkway and one step leading to the main entrance. The main entrance is a full-length glass-paned door trimmed in white with a gold-colored handle and door lock. There are two concrete planters in front of the home. There is no number on the premises but the odd-numbered units are sequential.





ATTACHMENT B

Property to be Seized

ITEMS TO BE SEIZED FROM THE PREMISES, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2251, 2252, 2252A, and 2423 from on or about January 1, 2019 to the present:

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252, 2252A, and 2423 in any form wherever they may be stored or found;

2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

   a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and

   b. electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

   c. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.

7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

8. Records evidencing occupancy or ownership of the PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Records or other items which evidence ownership or use of computer equipment found in the PREMISES, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.

11. Address books, names, lists of names and addresses of individuals believed to be minors.

12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors, including any notes or other records with or about the Victim and any photographs of her.

13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.

14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Any and all records, documents, invoices and materials that travel to the Philippines.

16. Any and all records, documents, and materials that concern the SUBJECT ACCOUNT.

17. Computers[2] or storage media[3] that contain records or information (hereinafter "COMPUTER") used as a means to commit violations of 18 U.S.C. §§ 2252 and 2252A. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252, 2252A, and 2423 from on or about January 1, 2019, including:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

---

[2] A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

[3] A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment;

18. Records and things evidencing the use of the Internet Protocol address 24.189.120.182, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. Internet Protocol addresses used by the COMPUTER;

c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

17. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein, all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252, 2252A, and 2423.